Overview

Chapter 2 examines the following issues:

- *how definitions of computer hacking and hackers are constructed and contested;*
- *how political, criminal justice and popular representations of hackers embody wider cultural concerns about technological and social change;*
- *the kinds of activities involved in hacking, and the tools and techniques used to undertake them;*
- *the realities behind the myth of hacking as an expert and elite activity;*
- *the ways in which various actors seek to account for and explain hackers' motivations for engaging in computer intrusions;*
- *the legal responses that have emerged in recent years in response to the perceived threat to society posed by hacking.*

key terms

Cracking
Denial of service
Differential association
Gender
Hacking
Malicious software or 'malware'
Masculinity
Subculture
Techniques of neutralization
Trojan horses
Viruses
Website defacement

Hackers and hacking: contested definitions

2.1 A few decades ago, the terms 'hacker' and 'hacking' were known only to a relatively small number of people, mainly those in the technically specialized world of computing. Today they have become 'common knowledge', something with which most people are familiar, if only through hearsay and exposure to mass media and popular cultural accounts. Hacking provides one of the most widely analysed and debated forms of cybercriminal activity, and serves as an intense focus for public concerns about the threat that such activity poses to society. Current discussion has coalesced around a relatively clear-cut definition, which understands hacking as 'the unauthorised access and subsequent use of other people's computer systems' (Taylor, 1999: xi). It is this widely accepted sense of hacking as 'computer break-in', and of its perpetrators as 'break-in artists' and 'intruders', that structures most media, political and criminal justice responses. Thus we would appear to have a fairly definite and unambiguous starting point for an exploration of this kind of cybercrime.

However, the term has in fact undergone a series of changes in meaning over the years, and continues to be deeply contested, not least among those within the computing community. The term 'hacker' originated in the world of computer programming in the 1960s, where it was a *positive* label used to describe someone who was highly skilled in developing creative, elegant and effective solutions to computing problems. A 'hack' was, correspondingly, an innovative use of technology (especially the production of computer code or programs) that yielded positive results and benefits. On this understanding, the pioneers of the Internet, those who brought computing to 'the masses', and the developers of new and exciting computer applications (such as video gaming), were all considered to be 'hackers' *par excellence*, the brave new pioneers of the 'computer revolution' (Levy, 1984; Naughton, 2000: 313). These hackers were said to form a community with its own clearly defined 'ethic', one closely associated with the social and political values of the 1960s and the 1970s' 'counterculture' and protest movements. This ethic emphasized, among other things, the right to freely access and exchange knowledge and information; a belief in the capacity of science and technology (especially computing) to enhance individuals' lives; a distrust of political, military and corporate authorities; and a resistance to 'conventional' and 'mainstream' lifestyles, attitudes and social hierarchies (Taylor, 1999: 24–6; Thomas, 2002). While such hackers would often engage in 'exploration' of others' computer systems, they purported to do so out of curiosity, a desire to learn and discover, and to freely share what they had found with others; damaging those systems while 'exploring', intentionally or otherwise, was considered both incompetent and unethical. This earlier understanding of hacking and its ethos has since been largely overridden by its more negative counterpart, with its stress upon intrusion, violation, theft and sabotage. Hackers of the 'old school' angrily refute their depiction in such terms, and use the term 'cracker' to distinguish the malicious type of computer enthusiast from hackers proper. Some would suggest that these differences are of little more than historical interest, and insist that the current, 'negative' and 'criminal' definition of hacking and hackers should be adopted, since this is the dominant way in which the terms are now understood and used (Twist, 2003). Moreover, to shift around between different groups' and individuals' definitions only invites confusion. There is considerable value to this pragmatic approach – throughout this and subsequent chapters, the 'terms 'hacking' and 'hackers' will be used in the current sense to denote those illegal activities associated with computer intrusion and manipulation, and to denote those persons who engage in such activities.

The contested nature of the terms is, however, worth bearing in mind, for a good criminological reason. It shows how hacking, as a form of cybercriminal activity, is actively *constructed* by governments, law enforcement, the computer security industry, businesses, and the media; and how the equation of such activities with 'crime' and 'criminality' is both embraced and challenged by those who engage in them. In other words, the contest over characterizing hackers and hacking is a prime example of what sociologists such as Becker (1963) identify as the 'labelling process', the process by which categories of criminal/deviant activity and identity are socially produced. Reactions to hacking and hackers cannot be understood independently from how their meanings are socially created, negotiated and resisted. Criminal justice and other agents propagate, disseminate and utilize negative constructions of hacking as part of the 'war on cybercrime'. Those who find themselves so positioned may reject the label, insisting that they are misunderstood, and try to persuade others that they are not 'criminals'; alternatively, they may seek out and embrace the label, and act accordingly, thereby setting in motion a process of 'deviance amplification' (Young, 1971) which ends up producing the very behaviour that the forces of 'law and order' are seeking to prevent. *In extremis*, such constructions can be seen to make hackers into 'folk devils' (Cohen, 1972), an apparently urgent threat to society which fuels the kinds of 'moral panic' about cybercrime alluded to in the previous chapter. As we shall see, such processes of labelling, negotiation and resistance are a central feature of ongoing social interactions about hacking.

Representations of hackers and hacking: technological fears and fantasies

2.2 This chapter began by noting that hacking comprises one of the most widely discussed areas of cybercriminal activity; indeed, for many people cybercrime and hacking have become synonymous. The public discourse on hacking appears to evoke fear and fascination in equal measure. The origins of this intense controversy can be understood in a number of different ways. The most straightforward explanation of social sensitivities to hacking stresses the degree of threat or danger that the activity carries. From what Hunt (1987) calls an 'objectivist' view of social problems, the response to hacking is a perfectly understandable and appropriate reaction to the level of social harm that it causes. The constant stream of estimates about financial losses incurred from hacking, and analyses of the dangers it poses to national security and public safety, would appear to give credence to such a view (see, for example, Coutorie, 1995; Bowers, 1998; Boni, 2001). Put simply, this viewpoint states that we are *right* to be extremely alarmed by hacking, because objective assessments show us that hacking *is* an extremely damaging form of cybercriminal behaviour. However, numerous commentators have suggested that social representations of the hacker threat are out of all proportion to the actual harm that their activities cause (Sterling, 1994; Kovacich, 1999). Thus official pronouncements on hacking often tend towards hyperbole – as, for example, when a senior law enforcement official told the US Senate that the nation is facing 'a cyber equivalent of Pearl

Harbor' (cited in Taylor, 1999: 7). Similarly exaggerated responses may be seen in media accounts. Taylor (1999: 7) recounts a story from a UK 'tabloid' newspaper depicting a 17-year-old computer hacker who, while ensconced in his bedroom, had supposedly broken into US military systems and had 'his twitching index finger hover[ing] over the nuclear button'. Such lurid and (literally) apocalyptic representations of hacking suggest that we have to look beyond the 'objective' assessment of threats if we wish to understand why it evokes such a heightened degree of alarm.

Paul Taylor (1999, 2000) situates social representations of hackers and hacking in the context of wider responses to rapid technological change. Historically speaking, such change has often incited anxieties that technology presents a threat to human existence, a fear that the more powerful our creations, the more they can escape our control and do untold damage. Thus, in Mary Shelley's *Frankenstein*, a scientist's desire to 'play God' and generate new life results in the creation of monster that turns on its creator. The theme of technological monstrosities, unwittingly unleashed by 'mad scientists', subsequently became a staple of twentieth-century popular culture (Tudor, 1989). From the 1960s onwards, the computer has come increasingly to the fore as the embodiment of this technological 'Pandora's box'. Thus, in Stanley Kubrick's *2001: A Space Odyssey* (1969) the initially benevolent spaceship computer HAL goes 'insane' and turns to murdering the human members of the crew. In the 1977 film *Demon Seed*, an experiment in artificial intelligence goes awry, creating a 'demonic' computer that even goes so far as to rape a woman in order to create its 'child', a human–machine hybrid. Similar themes are replayed in the popular *Terminator* series of films, in which a sentient military computer called Skynet launches a nuclear war against its human masters. Such representations, it can be suggested, give voice to a wider unease about technological innovation and its potentially uncontrollable catastrophic effects. Films focusing on hacking reinterpret such themes in their own particular way. The 1983 movie *War Games* tells the tale of a teenage hacker who unknowingly breaks in to a military computer and, while thinking he is playing a computer game called 'global thermonuclear warfare', brings the world to the very edge of nuclear oblivion. Such representations also point to a related kind of cultural anxiety, the fear that the more technologically oriented we become, the less human we are, the more we lose touch with a 'normal' existence. Representations of hackers (in both fiction and non-fiction) often allude to this, depicting them as alienated, dysfunctional and isolated loners who are able to interact effectively only with their computers. The fact that hackers are also invariably *young* in popular perceptions is also not a coincidence – the apparent ease with which a 'younger generation' is able to engage with the realm of computer technology, a technology that many older people continue to see as mysteriously daunting, merely serves to sharpen the sense that all manner of extravagant things may be possible for those with the know-how.

The sceptical reader may at this point object that the above examples are 'merely' Hollywood fictions, and that people are sufficiently astute to be capable of distinguishing them from 'reality'. However, such dismissal may overlook the profound ways in which popular representations shape public understandings of the world. Thus, for example, the aforementioned *War Games* was presented before a committee of the US Congress as an example of possible threats from hacking (as, a few years later, was the film *Die Hard II*, in which terrorists hack into an air traffic control computer in order to hold the authorities to ransom by threatening to crash incoming aircraft) (Taylor, 1999: 10). Law enforcement agencies have shown a similar willingness to make inferences about real-life hackers and their activities from depictions of their fictional counterparts (ibid.: 181). Taylor (ibid.: 9) concludes that 'the movies' representations of hacking have had a disproportionately important influence upon the legislative response to the activity' and that 'over-reliance upon fictional portrayals of hacking by the authorities has contributed to helping to create a generally fearful and ignorant atmosphere'. In short, cultural anxieties and their popular representation have played a significant role in how the threat from hacking has come to be perceived in both official and wider public domains.

However, social representations of hackers and hacking have not been exclusively of a negative kind. Rather, they exhibit considerable ambivalence, with hackers evoking a kind of fascination and even admiration. Studies of public attitudes suggest that among a significant portion of the population, especially the young, hackers and their activities are viewed in a rather positive light (Dowland et al., 1999: 720; Voiskounsky et al., 2000: 69–76). There are a number of ways in which such favourable representations of hacking can be understood. First, they can be seen in relation to the aforementioned sense of threat or anxiety evoked by new and seemingly incomprehensible technologies. In such a situation, hackers come to represent a mastery of the arcane new world of computing that others desire or aspire to. Consequently, public perceptions of hackers often stress traits such as unusual intelligence and ingenuity (Voiskounsky et al., 2000: 72–3); news media also propagate similar images of hackers as 'genuises', 'wizards' and 'virtuosos' (Furnell, 2002: 201). Depictions of hacking as arcane, mysterious and powerful also appear in popular fictions. For example, the sci-fi thriller *The Core* (2003) features a brilliant hacker who demonstrates his abilities to a sceptical audience by 'hacking' a mobile phone by merely whistling tones into the handset through a foil gum wrapper; finishing this 10-second piece of hacker virtuosity, he laconically hands the phone back to its owner, claiming that 'You now have free long-distance calls for life!'. The implication here is that, while hackers are seen as threatening insofar as they immerse themselves in an 'alien' and dehumanized world of technology, they also offer a vision of individuals reclaiming their autonomy by taking forceful control of a technological system which they can use for their own human ends (Taylor, 2000: 43). A second kind of threat, to which hackers appear to offer resistance, is the perceived domination of high technology by governmental powers and/or faceless corporations. Concerns about the Internet often coalesce around a kind of Orwellian nightmare of surveillance and manipulation, and hackers are sometimes represented as the resistance to such unaccountable and invasive uses of technological power – what one commentator dubs the 'freedom fighters of the 21st century' (Kovacich, 1999). Popular culture again appropriates and disseminates such interpretations. The film *Hackers* (1995), for example, portrays an idealistic group of young computer outlaws who use their hacking skills to take on corporate conspirators who are intent on causing an ecological catastrophe, which they will blame on our innocent 'heroes'. In a similar vein, public resentments about the domination of computer technology by corporations such as Microsoft are explicitly exploited in *AntiTrust* (2001), another computer crime movie. Here, a (thinly disguised) Bill Gates-like computer tycoon is hell-bent on global domination at any cost, only to be thwarted by young computer 'geeks' who hold fast to the 'hacker ethic' of freedom of information and knowledge. In sum, we can see that socio-cultural fears and fantasies about computer technology shape often ambivalent and contradictory representations of the hacker, who appears as 'a schizophrenic blend of dangerous criminal and geeky Robin Hood' (Hawn, 1996; cited in Taylor, 2000: xii).

What hackers actually *do*: a brief guide for the technologically bewildered

2.3 Having examined the contested definitions and wider representations of hackers and hacking, it is now time to consider in a little detail what it is that hackers actually do when they 'hack', and how they go about it. As will become apparent below, 'hacking' is, in fact, a generic label for a range of distinct activities associated with computer intrusion, manipulation and disruption.

Unauthorized access to computer systems

2.3.1 The most fundamental form of hacker activity is that of gaining access to, and control over, others' computer systems. Once such access and control have been gained (what hackers call 'taking ownership' of a system), a range of further prohibited activities become possible. Such access is made possible by the networking of computer systems, since their inter-connection makes it possible to access a system from the 'outside', from other computers which can connect to it. The Internet has increased the possibilities for such intrusion many-fold since, given the network's 'open architecture', all systems connected to it are 'public facing', i.e. can be communicated with remotely by anyone who can establish an Internet connection (Esen, 2002: 269). As an ever-greater number of systems have become connected to the Internet, the number of such intrusions has increased steadily. For example, in 1998 the FBI reported that computer intrusion incidents had increased 250 per cent over a two-year period (Lilley, 2002: 32). In 2003, 36 per cent of US organizations questioned in the annual CSI/FBI computer crime survey reported having experienced a 'system penetration' attack. The Internet was reported as an increasingly frequent point of attack, with 78 per cent of respondents reporting at least one such incident in the previous 12 months, up from 57 per cent in 1999 (CSI/FBI, 2003: 8–10). The frequency of such intrusions is anticipated to continue rising markedly, as Internet use continues to spread, and an ever greater range of Internet-enabled devices become available (such as personal digital assistants (PDAs) and mobile phones). Moreover, given that as few as 5 per cent of incidents are thought to actually be reported to the authorities (Lilley, 2002: 32), the extent of such intrusions may well be massively greater than official figures reveal.

Illegalities following computer intrusion

2.3.2 Once access to a computer system has been established, hackers are able to perpetrate a further range of criminal acts. These include the following:

- *Theft of computer resources.* Hackers may use the resources of the hacked system for their own purposes, such as the storage of illegal or undesirable materials. In one such incident a hacker from Sweden illegally accessed an American university's systems, and used them to store and distribute a massive array of pirated music (MP3) files (Furnell, 2002: 101).
- *Theft of proprietary or confidential information.* Hackers may exploit unauthorized access in order to steal or copy information including software, business secrets, personal information about an organization's employees and customers, and credit card details which can subsequently be used for fraudulent purposes. Theft of proprietary information is cited as the greatest source of financial losses by business and other organizations (CSI/FBI, 2003: 4). There have even been cases in which seemingly reputable business organizations have allegedly commissioned hackers to steal confidential information from their competitors (Eichenwald, 1998: 157). Incidents also abound in which thousands of customer credit card details have been stolen as a result of hacking incidents, or in which hackers were able to exploit banks' systems to arrange illegal electronic transfers of funds (Riem, 2001: 12–13; Travis, 2001; Wilding, 2003: 4). In one case of the former, a Russian hacker known only as 'Maxim' accessed the systems of an Internet retailer and stole details of some 300,000 credit cards; when the company refused to pay the $100,000 the hacker demanded as part of 'his' blackmail scheme, 'he' posted details of

25,000 of the cards on the Internet (Philippsohn, 2001: 57). In an instance of the latter, a group of hackers, again from Russia, managed to electronically transfer over $10 million from the accounts of Citibank's US customers (Grabosky and Smith, 2001: 34).

- *Systems sabotage, alteration and destruction.* Hackers may exploit access to cause significant amounts of damage to a system's operations. While outright 'trashing' of content is relatively rare (Furnell, 2002: 101), it is not unheard of; there have been a number of documented cases in which disgruntled former employees have unleashed such destruction upon their erstwhile employers in revenge for having been dismissed (Philippsohn, 2001: 55). More frequent is the selective alteration of data held within the system. This may be undertaken by hackers so as to cover their tracks, hiding from administrators the fact that their system has been compromised, thereby allowing the hackers to access the system on an ongoing basis. Systems content may be also be altered or erased by hackers 'as a prank, protest, or to flaunt their skills' (Denning, 1999: 227). (Tampering as a protest or political act will be considered in detail in Chapter 3). Hackers may also alter data so as to gain some personal advantage for themselves, their friends or family. There are a number of cases in which students gained access to school or university computers to alter their own or their friends' grades. There was even one incident in which an inmate of a California jail broke into the prison's information system, and altered his release date 'so that he could be home in time for Christmas' (ibid.,). Overall, some 21 per cent of organizations surveyed in the USA report having experienced some such form of sabotage during a 12-month period (CSI/FBI, 2003: 10); in the UK for the same period, 'sabotage of data or networks' was estimated to have impacted upon 9 per cent of business organizations (NOP/NHTCU, 2002: 4).
- *Website defacement and 'spoofing'.* Such hacker attacks directly target Internet websites themselves, and can take a number of distinct forms. In instances of 'defacement', the website is hacked and its contents altered. These may be viewed as 'pranks' intended to 'amuse' web-surfers, as exercises in self-aggrandizement by hackers who wish to advertise their skills, or as ideologically and politically motivated forms of protest against governments and businesses (Vegh, 2002; Woo et al., 2004). Website defacements are an increasingly prominent form of hacker activity, with recorded attacks rising from just 5 in 1995 to almost 6000 in 2000 (Furnell, 2002: 104). Victims in recent years have included the US, Hong Kong, and Colombian governments, the CIA and the US military, the UK Labour and Conservative Parties, the *New York Times*, the LAPD, as well as (ironically) the sites of companies specializing in providing Internet security solutions (Denning, 1999: 228–31; Furnell, 2002: 103–9; Lilley, 2002: 53–4). The second form of website-centred hack, 'spoofing' does not attack organizations' actual sites. Rather, the hacker establishes a 'spoof' or 'fake' website to which the unsuspecting Internet user is re-directed. Again, this can cause considerable embarrassment to the owner of the legitimate website, since its forged replacement may feature offensive speech, pornographic imagery, or accusations about the victim's supposedly unsavoury business or political practices. Spoofing is also used in the commission of Internet

frauds. In such cases, the forged website is made to appear as similar as possible to its legitimate counterpart, so that the visitor may be unaware that it is a fake. The user will thus proceed to use the site as normal, for example, by attempting to log on using their username and password. In the case of e-commerce and e-banking sites, for example, this has been exploited to acquire access to customers' accounts which can then be raided (Philippsohn, 2001: 60). (Website spoofing for the commission of fraud will be considered further in Chapter 5).

In addition to those activities outlined above, there are a number of important, illicit activities usually associated with hacking, but which do not in fact require unauthorized access or 'break-in' to a computer system; rather, they can be engineered simply via email or Internet connection:

- *Denial of service attacks.* 'Denial of service' basically refers to a cyber-attack 'which prevents a computer user or owner access to the services available on his system' (Esen, 2002: 271). Such an attack can be performed without direct access to a system, by 'flooding' Internet-accessible computers with communications, so that they become 'overloaded' and are rendered unable to perform functions for legitimate users. Such attacks are seen as an increasingly frequent form of hacker activity, with 42 per cent of US-based and 20 per cent of UK-based organizations reporting such attacks during 2002–3 (CSI/FBI, 2003: 10; NOP/NHTCU, 2002: 4). During 2001, in one of the most publicized cases of recent years, a 15-year-old Canadian, going under the hacker pseudonym of 'Mafiaboy', managed to effectively shut down access to leading e-commerce websites such as Amazon.com and eBay.com, as well as the site of the global news service CNN. At his subsequent trial, he was alleged to have caused some $1.7 billion in damages (BBC News, 2001a).
- *Distribution of 'malicious software'.* Malicious software (or 'malware' for short) refers to computer codes and programs, usually distributed via the Internet and email, which infect computers, causing varying degrees of disruption to their operation or damage to data. Malware takes a number of distinctive forms, such as 'viruses', 'worms' and 'Trojan horses'. Computer viruses, like their biological counterparts, need hosts to reproduce and transmit themselves (Boase and Wellman, 2001: 39). Worms, however, are independent pieces of software capable of self-replication and self-transmission (for example, by emailing themselves to others in a computer's address book) (Furnell, 2002: 147). A Trojan horse, as the name suggests, is a program that appears to perform a benign or useful function, but in fact has some hidden destructive capabilities that only become apparent after a user has downloaded and installed the software. Taken together, such forms malware are widely recognized as the most disruptive and destructive kind of cyber-attack (CSI/FBI, 2003: 4). Chapter 1 began with the example of the 'Love Bug' worm that affected millions of computers in May 2001, causing an estimated 7–10 billion dollars of damage. A few months later, on 13 July, the 'Code Red' worm appeared, and infected more than a quarter of a million systems in its first nine hours (CERT/CC, 2002). By 1 August, it had caused an estimated $1.2 billion in losses (BBC News,

01/08/01). In January 2004, a virus dubbed 'MyDoom' became the fastest spreading virus ever, causing an estimated $20 billion of damage to businesses worldwide in just 15 days (Wright, 2004; McCandless, 2004). As I write this, the 'Sasser' worm is in its second week of release, and has already infected millions of machines, including the systems of the South African government, the UK coastguard, the Taiwanese national post office, and the Australian rail network (leaving some 300,000 passengers stranded) (Sophos, 2004). The massive disruption caused by such malicious codes is a consequence of the way in which they can use the Internet to rapidly distribute themselves – the openness of the network and the near-instantaneity of communication enable them to replicate and spread exponentially. Further problems arise as viruses, again like their biological equivalents, are often capable of mutation, thereby evading virus detection and eradication systems programmed to recognize only earlier versions of the code (Boase and Wellman, 2001: 41–2). A piece of malware need be sent to only a single networked machine from which it can automatically spread to millions of others without any further action from its author. This capacity for generating rapid and widespread disruption to the global network of computer systems is now viewed as a key tool for conducting 'information warfare', 'cyberterrorism' and other politically motivated attacks (considered in detail in Chapter 3).

2.4 Hacker myths and realities: wizards or button-pushers?

In Section 2.2, I noted the tendency of social representations of hacking to stress the technical virtuosity and exceptional abilities of its practitioners. Press reporting has propagated such imagery, not least because it enhances the frisson of danger and fascination surrounding the activity, creating around the figure of the hacker a kind of mystique. Popular fiction has similarly stressed the abnormal intelligence and skills of hackers – in films such as *Hackers*, *The Core* and *The Italian Job* (2003), the hacker appears as a kind of savant, using knowledge and techniques far beyond the comprehension of normal people to achieve the most awe-inspiring control over computerized systems. Such cultural constructions of the hacker as a 'genius' have significantly shaped wider perceptions of hacking as a social practice. If such perceptions are valid, then the actual number of hackers may be very limited, given that only the most gifted and accomplished can acquire the skills necessary to succeed. Estimating numbers is particularly difficult, given the inherently covert nature of the activity, the increasing criminal sanctions that can be brought to bear upon hackers if identified and which serve to drive them further underground, and the capacity for anonymity afforded by the Internet environment. Writing in the relatively early days of mass-networked computing, Sterling (1994: 76–7) estimated that the 'digital underground' of hacking comprised no more than about 5,000 individuals, of whom 'as few as a hundred are truly "elite" – active computer intruders, skilled enough to penetrate sophisticated systems and truly to worry corporate security and law enforcement'. More recently, TruSecure, a US-based Internet security company, is aware of some 11,000 individuals organized into about 900 different hacking groups (Twist, 2003). While the numbers may have increased over the past decade, the levels of skill and knowledge necessary for effective hacking appear to present a barrier to entry, thereby setting limits on the extent of hacking as a cybercrime problem.

However, the view of hacking as an activity restricted to a small, highly able and motivated 'elite' may be increasingly at odds with reality. Hacking itself has undergone considerable evolution and change over recent years. Perhaps it was true that, for an earlier generation of hackers, crackers and viral-coders, technical knowledge and skills were a prerequisite, since they had to rely on either formal training in computing and/or concerted experimentation, trial and error in order to stage attacks. However, as hacking techniques have evolved, an increasing range of automated software tools have appeared which can perform much of the necessary work. For example, the kinds of unauthorized access and hijacking of computers described earlier can now be performed with a range of tools such as 'Titan', 'SATAN', and 'BO2K' which probe networks to find vulnerable systems and establish remote control over them; programs such as 'Ethereal' and 'L0phtCrack' can be used to capture and decrypt user passwords (Furnell, 2002: 119). Similarly, denial of service attacks can now be launched automatically using software such as 'FloodNet' (Denning, 1999: 237). Such tools are readily available for download from hacker websites. There are also numerous readily available tools for creating viruses and worms (over 100 according to one estimate). Many of these programs come with user-friendly Windows-style interfaces, pull-down menus and even 'help' files to guide the inexperienced user. One such tool, the 'Vbs Worm Generator', allows the user to custom-design a worm with a range of different destructive payloads, all with a few clicks of the mouse (Furnell, 2002: 178–81). Such tools enable even the novice, with little or no existing expertise, to generate cyber-attacks. Thus in 2001, a 20-year-old from the Netherlands, calling himself 'OnTheFly', used the Vbs tool to create the 'Anna Kournikova' worm. When it spread across the Internet with alarming and unexpected rapidity, the terrified author surrendered himself to the authorities. He subsequently revealed that it was his first effort at viral coding and 'it only took me a minute to write it' (Delio, 2001). In the words of 'Sir Dystic', one of the authors of the 'BO2K' hacking tool, 'we made the software easy enough for an eight-year-old to hack with and we think it could do serious damage' (cited in Furnell, 2002: 123). Such technical innovations have effectively 'democratized' hacking, making it increasingly available to anyone with a PC, Internet connection and the curiosity or desire to see if they too can join the 'digital underground'.